

Appl. No.: 10/015,826  
Amdt. Dated October 27, 2005  
Response to Office Action of July 26, 2005

#### REMARKS/ARGUMENTS

Claims 1-29 are currently pending in the present application. Claims 1-14 have been rejected under 35 U.S.C. § 112, second paragraph, as allegedly being indefinite. Claims 1-29 have been rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over U.S. Patent No. 6,829,709 to Acharya et al. in view of U.S. Patent No. 6,366,563 to Weldon et al. and U.S. Patent No. 6,795,917 issued to Ylonen et al. Applicants respectfully traverse the rejections.

To overcome the rejection under 35 U.S.C. § 112, Applicant has amended claim 1 to replace "identified" with "discovered." Applicant submits that the foregoing amendment overcomes the rejection under 35 U.S.C. § 112, and respectfully requests withdrawal thereof. In addition, Applicant respectfully requests entry of the foregoing amendment to place the claims in better form for reconsideration, or for consideration upon possible appeal of the instant rejections.

Applicant respectfully requests reconsideration of the Examiner's rejection under 35 U.S.C. § 103(a) based on the combination of Acharya, Weldon and Ylonen. As set forth below, it is clear that the combined teachings of the foregoing references fail to disclose or suggest the claimed subject matter. To summarize, the Examiner admits that neither Acharya nor Weldon teach probing of a communications path to a destination to discover a network address of a network device having compatible transformation tunnel capabilities. See Office Action at page 4, paragraph 15. The Examiner's reliance on Ylonen to supply this missing subject matter is unfortunately misplaced, as Ylonen provides no such teaching. Indeed, as discussed below, Ylonen suggests that the network address of the tunnel partner with which it exchanges probe messages is known, not discovered. Furthermore, the probe messages taught in Ylonen are transmitted to identify whether the packets exchanged with a known tunnel partner undergo any address translations or protocol conversions that may affect operation of message authentication mechanisms. Ylonen, however, does not disclose the use of probe messages to discover a tunnel partner.

Applicant has previously amended independent claims 1, 15, 22 and 29 to state that the communications path to destination hosts are probed to discover the network addresses of network devices having compatible transformation tunnel capabilities. These network

Appl. No.: 10/015,826

Amdt. Dated October 27, 2005

Response to Office Action of July 26, 2005

addresses can be used to establish tunnels with the discovered network devices. None of the cited references disclose or suggest the probing of a communications path to a destination host to dynamically discover the network address of a network device in the path that has compatible transformation tunnel capabilities. In contrast to the claimed subject matter, the cited references teach systems where the network address information is manually configured, or are silent as to how such network address information is obtained. For example, Acharya teaches methods and systems that validate that network traffic transformation mechanisms--such as encryption, encapsulation, and network address translation--, have been properly configured. See '709 Patent, Col. 2:43-54. As Acharya states, the validation process validates that the transformation process is performing properly on the IP tunnel between two devices. '709 Patent, Col. 6:8-10. Essentially, a validation client at one network sends a sequence of messages to a validation daemon at another network participating in the IP tunnel. The validation daemon inspects the received messages to ensure that the transformation process of the IP tunnel is functioning properly. Acharya, Col. 6:10-23; col. 6:33-62. Acharya, however, contains no mention of how the network devices at each end of the IP tunnel are configured with the network address information required to conduct the validation. Rather, Acharya appears to assume that each network device has been configured with the network address at the opposite side of the IP tunnel.

Similarly, Weldon does not teach a system that discovers the network address of network devices having compatible transformation tunnel capabilities. Indeed, Weldon teaches that the network address information for devices to be probed is manually configured. See '563 Patent, Col. 7:44-55 ("A Probe Poll List is maintained as an ASCII text file. ... Additional probes can be configured directly through a configuration edit display. Through the menu options for this screen, the user can add, delete or import probes to the Probe Poll List."). Furthermore, the system of Weldon uses probes to determine SLA compliance and network performance statistics. Still further, the Examiner's contention that Weldon discloses detecting a data flow to a destination host and probing the path to the destination host is unsupportable.

Lastly, Ylonen fails to disclose or suggest a system that discovers the network address of network devices in a communications path having compatible transformation tunnel

Appl. No.: 10/015,826

Amdt. Dated October 27, 2005

Response to Office Action of July 26, 2005

capabilities. Rather, Ylonen discloses packet authentication in network environments that include network address translation and protocol conversion in the path between the participating nodes in an IPSEC tunnel. Ylonen's object is to provide a packet authentication method that is insensitive to address translation and protocol conversions. See Ylonen, Col. 3:66-Col. 4:1. Ylonen teaches a system where a first tunnel endpoint transmits probe packets to a known second tunnel endpoint to determine whether other devices in the communications path perform network address translation or protocol conversions. The second tunnel endpoint receives the probe packet and transmits it back to the first tunnel endpoint. The first tunnel endpoint compares the probe packet as received by the second tunnel endpoint to the probe packet that was transmitted. As Ylonen teaches, the first tunnel endpoint can use the discovered protocol conversions or network address translations to compute an authentication code (MAC) to enable the second tunnel endpoint to validate the encrypted packets. However, as with the other cited references, Ylonen does not teach the dynamic discovery of a tunnel endpoint; rather, it appears to be assumed that the tunnel endpoints have been manually configured with knowledge of each other. In fact, Ylonen itself appears to show that the tunnel peer address is known not discovered. See Ylonen, Col. 14:24-30.

Applicant also specifically addresses certain of the Examiner's allegations in the office action of July 26, 2005.

As to paragraph 16 of the Office action, the Examiner alleges that Weldon provides a motivation to achieve the allegedly invalidating combination of Acharya, Weldon and Ylonen. However, the use of "boilerplate" language that the invention is capable of being practiced in a number of different ways (see Weldon, Col. 12:34-39) is specious and not well-taken.

As to paragraph 17 of the Office Action, the Examiner incorrectly characterizes the teachings of Ylonen. Ylonen's object is to provide a packet authentication method that is insensitive to address translation and protocol conversions in the communications path between two known tunnel end points. Ylonen, Col. 3:66-Col. 4:1. Ylonen identifies the address translations and protocol conversions that occur on the path between two nodes. At Col. 4:22-36, Ylonen describes discovery of the address translations and protocol conversions that occur

Appl. No.: 10/015,826  
Amdt. Dated October 27, 2005  
Response to Office Action of July 26, 2005

between the end nodes of the tunnel, and the compensation of such discovered address translations and protocol conversions to allow the transmitted packets to be authenticated at the receiving end. However, the probe messages are not intended to be used by one endpoint to discover another endpoint. Rather, the probe messages of Ylonen require that each end point know the network address of each other. For example, at Col. 5:62-Col.6:7, Ylonen states that, to discover the transformations, the tunnel peers send probe packets between them and analyze the received packets to identify what transformations, if any, occur. Furthermore, at Col. 13:56-67, Ylonen teaches how the tunnel end points signal each other to say that probes have been received, and how each peer obtains information to figure out what address translations and protocol conversions occur on the communications path.


As to paragraph 18, the Examiner fails to establish an appropriate motivation or suggestion to combine the references. For example, the Examiner in part relies on an incorrect characterization of Ylonen's teachings. Furthermore, that Weldon teaches a central configuration platform to distribute configuration information to various VPN nodes (that exchange messages to determine SLA compliance), does not provide sufficient motivation to combine the teachings of Ylonen with Weldon and/or Acharya.

In light of the foregoing, Applicant believes that all currently pending claims are presently in condition for allowance. Applicant respectfully requests a timely Notice of Allowance be issued in this case. If the Examiner believes that any further action by Applicant is necessary to place this application in condition for allowance, Applicants request a telephone conference with the undersigned at the telephone number set forth below.

Date: October 27, 2005

Customer Number: 30505  
Law Office of Mark J. Spolyar  
38 Fountain St.  
San Francisco, CA 94114  
415-826-7966  
415-480-1780 fax

Respectfully Submitted,  
LAW OFFICE OF MARK J. SPOLYAR  
By

  
Mark J. Spolyar  
Reg. No. 42,164